FOS 5.6 What's New Deep Dive

R. Kříž

28.6.2017

Agenda

- ✓Flow Mode Changes
- ✓Proxy Mode Changes
- ✓VPN Changes
- ✓Routing Changes
- ✓Other Features

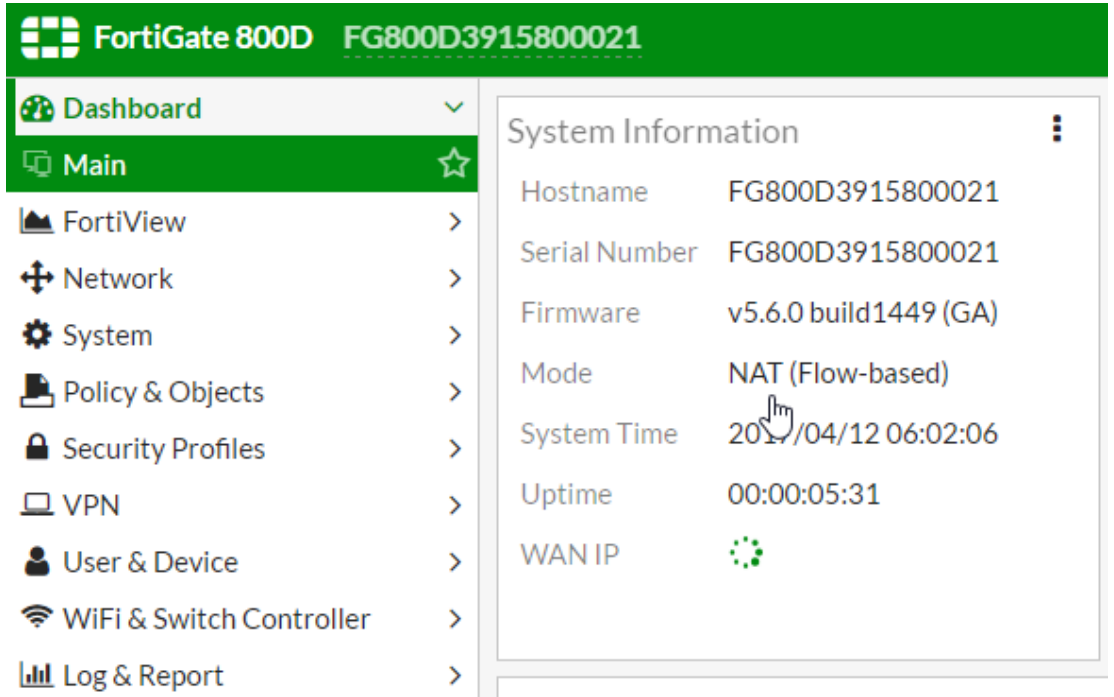
FortiOS V5.6 Platform Support

	5.2.10	V5.4.4	5.6
FG/FWF-20/40C/60C Series	✔		
FG/FWF-30D Series	✔	✔	✔
FG/FWF-30E/50E Series		✔	✔
FG/FWF-60E		✔	✔
FG/FWF-60D Series	✔	✔	✔
FG-70D Series	✔	✔	✔
FG/FWF-80C Series	✔	✔	✔
FG-80D	✔	✔	✔
FG-80E Series		✔	✔
FG/FWF-90D Series	✔	✔	✔
FG-90E Series		✔	✔*
FG/FWF-92D Series	✔	✔	✔
FG-100C Series	✔		

	5.2.10	5.4.4	5.6
FG-100D Series	✔	✔	✔
FG-100/101E		✔	✔
FG-200D Series	✔	✔	✔
FG-200/201E		✔	✔*
FG-300C	✔		
FG-300D/400D/500D/600D	✔	✔	✔
FG-600C/800C/1000C	✔	✔	✔
FG-800D/900D/1000D Series	✔	✔	✔
FG-2000E Series		✔	✔*
FG-3240C/3600C	✔	✔	✔
FG-3000D Series	✔	✔	✔
FG-5001C/50001D	✔	✔	✔
FG-7040E		✔	✔*

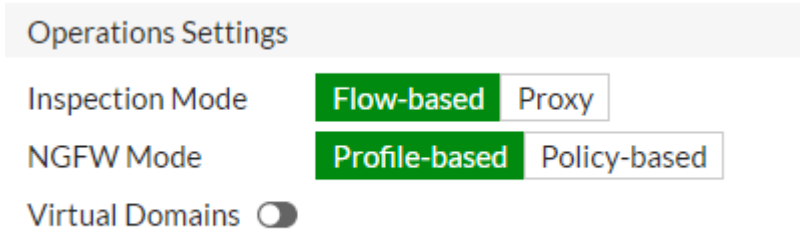
Flow Mode Changes

Default inspection Mode is FLOW



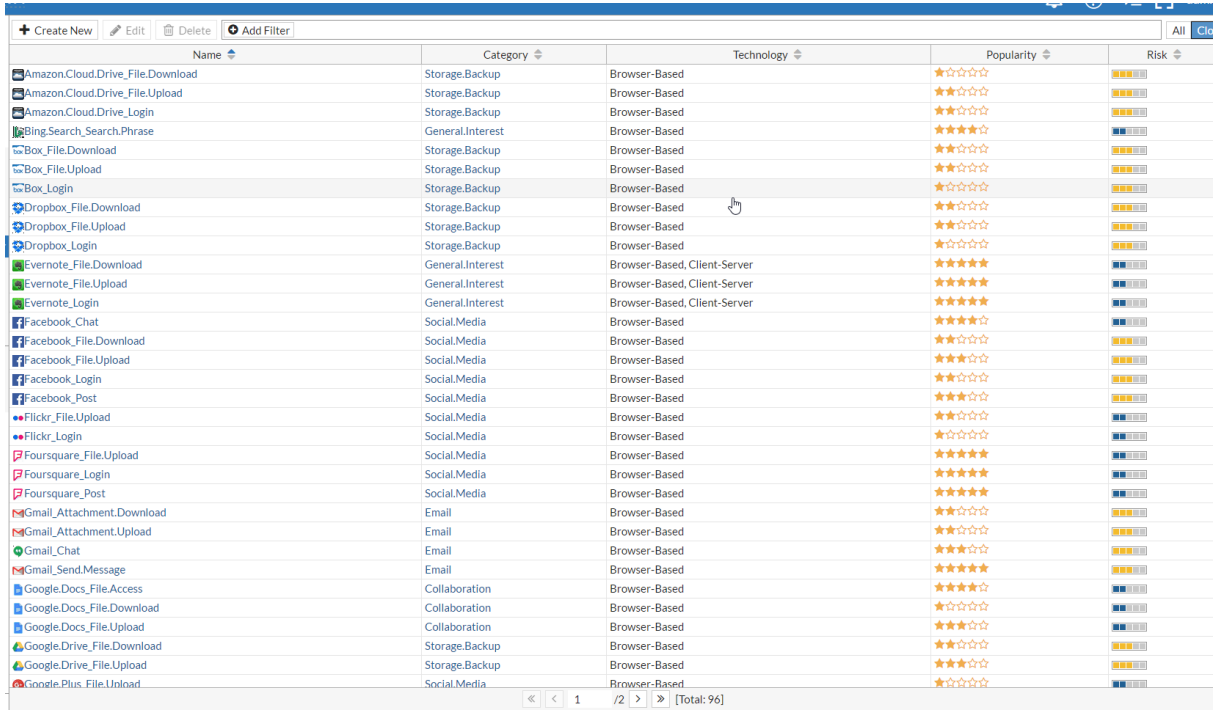
- Why
  - » Flow mode is benefiting from Nturbo which gives a boost in performance. To allow customer to benefit this, default mode changed from Proxy to Flow.
  - » Attention, for backward compatibility, CLI default option is still Proxy based but when you have a factory reset fortigate, the inspection will be flow based.

NGFW Mode



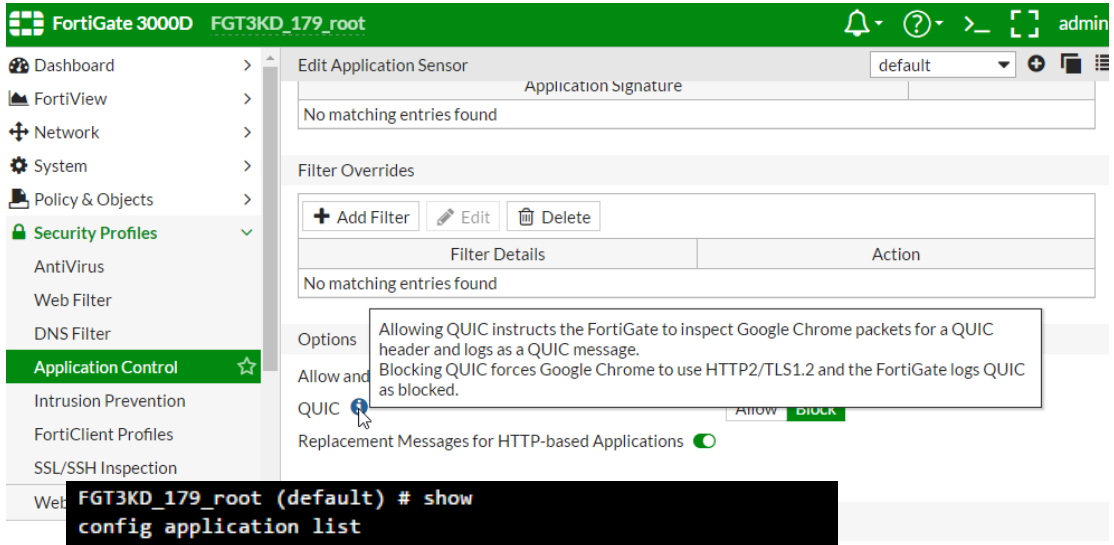
- Why
  - » To be competitive with Market requirement.
  - » You need to use Central NAT table & global SSL/SSH profile per VDOM

Merge CASI to application control



- CASI now part of appcontrol

Block QUIC default App-control




```
FGT3KD_179_root (default) # show
config application list
    edit "default"
        set comment "Monitor all applications."
        config entries
            edit 1
                set action pass
            next
        end
    next
end

FGT3KD_179_root (default) # set options
allow-dns     Allow DNS.
allow-icmp    Allow ICMP.
allow-http    Allow generic HTTP web browsing.
allow-ssl     Allow generic SSL communication.
allow-quic    Allow QUIC.
```

- What is QUIC

  - **QUIC** is the name for a new experimental protocol, and it stands for **Quick** UDP Internet Connection. The protocol supports a set multiplexed connections over UDP, and was designed to provide security protection equivalent to TLS/SSL, along with reduced connection and transport latency.

Split IPS and Appcontrol signatures

```
Attack Definitions
---------
Version: 10.00120
Contract Expiry Date: Fri Sep  8 2017
Last Updated using scheduled update on Thu Apr 13 18:56:34 2017
Last Update Attempt: Thu Apr 20 11:59:52 2017
Result: No Updates

Attack Extended Definitions
---------
Version: 10.00107
Contract Expiry Date: Fri Sep  8 2017
Last Updated using scheduled update on Thu Apr  6 18:58:48 2017
Last Update Attempt: Thu Apr  6 18:58:48 2017
Result: Updates Installed

Application Definitions
---------
Version: 10.00119
Contract Expiry Date: Fri Sep  8 2017
Last Updated using scheduled update on Thu Apr 13 18:56:34 2017
Last Update Attempt: Thu Apr 20 11:59:52 2017
Result: No Updates

Industrial Attack Definitions
---------
Version: 6.00741
Contract Expiry Date: n/a
Last Updated using manual update on Tue Dec  1 02:30:00 2015
Last Update Attempt: Thu Apr 20 11:59:52 2017
Result: Unauthorized
```

- Application Control signatures are now link to Forticare
- Industrial signatures (app-control and IPS) are now separated and they require service contract

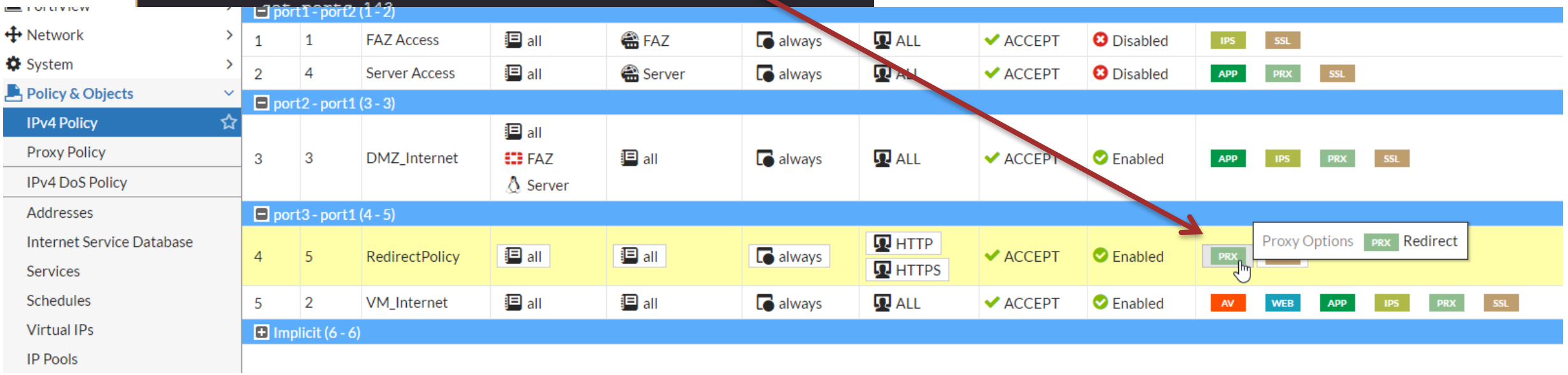
Proxy Mode Changes

Proxy VDOM

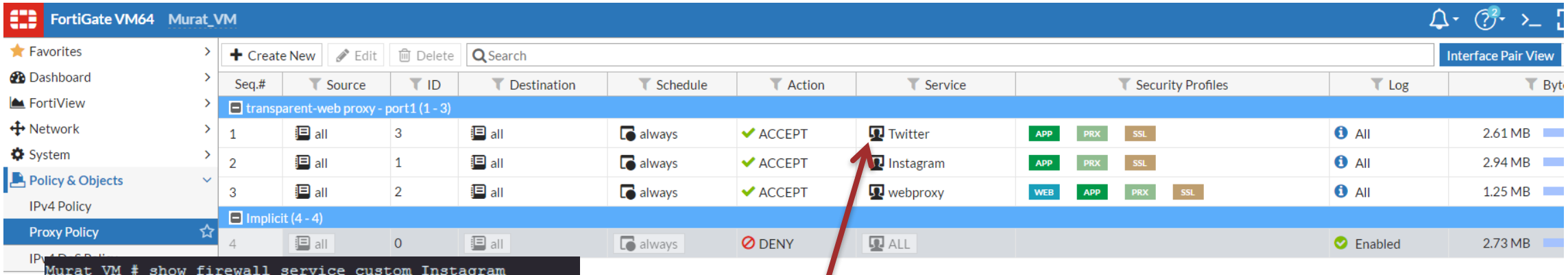
Transparent Proxy and Firewall

```
Murat_VM # show firewall profile-protocol-options Redirect
config firewall profile-protocol-options
    edit "Redirect"
        config http
            set ports 80
            unset options
            set http-policy enable
            unset post-lang
        end
        config ftp
            set ports 21
            unset options
        end
        config imap
```

This option is to redirect HTTP and HTTPS Traffic to Proxy Policy



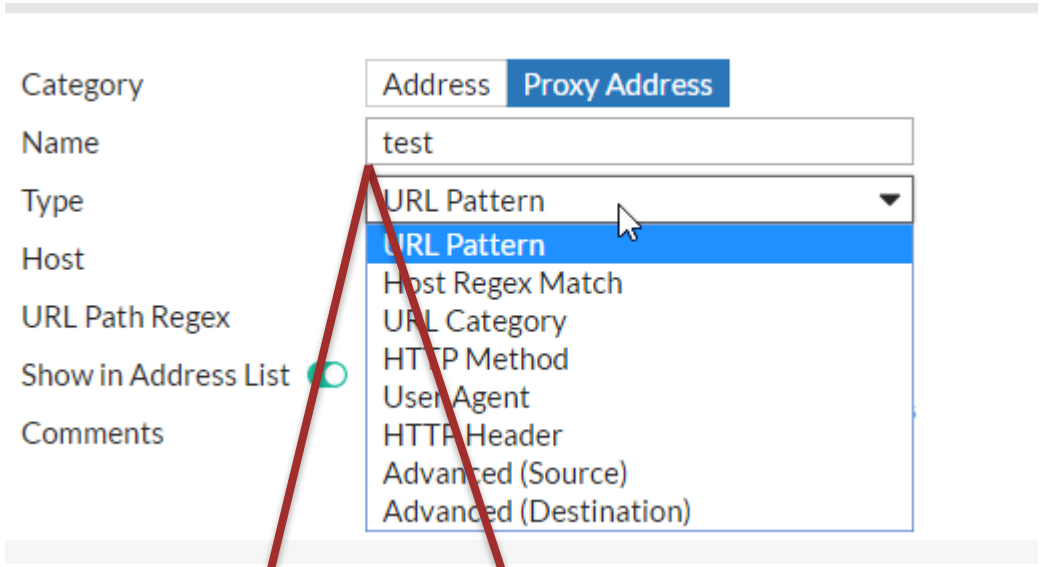
Proxy Policies




```
Murat_VM # show firewall service custom Instagram
config firewall service custom
    edit "Instagram"
        set explicit-proxy enable
        set protocol ALL
        set app-service-type app-id
        set application 34527
        set tcp-portrange 0-65535:0-65535
    next
end

Murat_VM # show firewall service custom Twitter
config firewall service custom
    edit "Twitter"
        set explicit-proxy enable
        set protocol ALL
        set app-service-type app-id
        set application 16001
        set tcp-portrange 0-65535:0-65535
    next
end
```

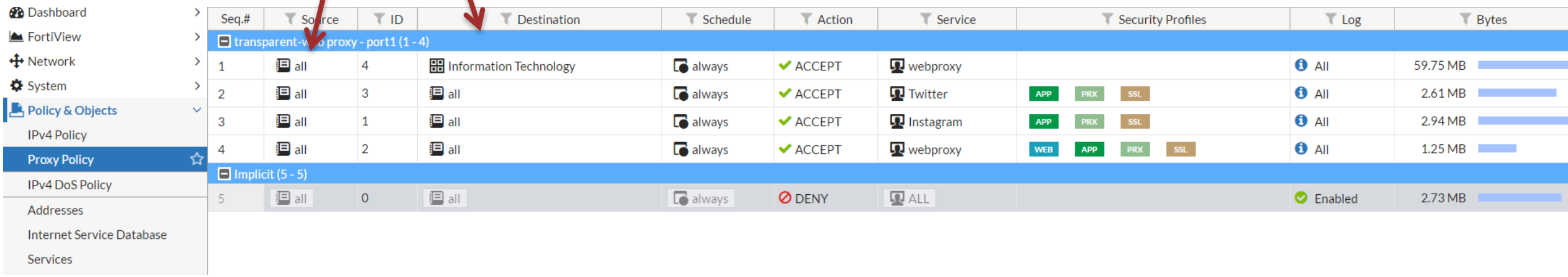
Application id selection is per Explicit Proxy Service

Source / Destination



Source and Destination Proxy Address objects are based on type

For example User agent can be source only Where URL category destination only



Internet Service database on Proxy Policies

```
Murat_VM (4) # show full-configuration
config firewall proxy-policy
    edit 4
        set uuid c8134fc0-2056-51e7-267a-2dd39b18ac5e
        set proxy transparent-web
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set internet-service enable
        set internet-service-negate disable
        set srcaddr-negate disable
        set action accept
        set status enable
        set schedule "always"
        set logtraffic utm
        set transparent disable
        set webcache disable
        set disclaimer disable
        set utm-status disable
        set replacemsg-override-group ''
        set logtraffic-start disable
        set scan-botnet-connections disable
        set comments ''
    next
end

Murat_VM (4) # set internet-service
internet-service           Enable/disable use of Internet Services for this policy. If enabled, destination address and service are not used.
internet-service-negate    When enabled internet-service specifies what the service must NOT be.
internet-service-id        Internet Service ID.
internet-service-custom    Custom Internet Service Name.
```

- Idea is using Internet service database as destination address object

OCSP support for SSL Deep inspection (Proxy mode)

```
Murat_VM (setting) # get
ocsp-status          : disable
ssl-ocsp-status      : disable
ssl-ocsp-option      : server
ocsp-default-server :
check-ca-cert        : enable
strict-crl-check     : disable
strict-ocsp-check    : disable
certname-rsa1024     : Fortinet_SSL_RSA1024
certname-rsa2048     : Fortinet_SSL_RSA2048
certname-dsa1024     : Fortinet_SSL_DSA1024
certname-dsa2048     : Fortinet_SSL_DSA2048
certname-ecdsa256    : Fortinet_SSL_ECDSA256
certname-ecdsa384    : Fortinet_SSL_ECDSA384

Murat_VM (setting) # set ssl-ocsp-status
enable      Enable SSL OCSP.
disable     Disable SSL OCSP.

Murat_VM (setting) # set ssl-ocsp-status enable

Murat_VM (setting) # set ssl-ocsp-option
certificate     Use URL from certificate.
server          Use URL from default OCSP server.
```

- This allows Fortigate validate the revoked certificates via OCSP
- When certificate is revoked, Deep inspection will sign the self generated server certificate with Fortinet_CA_Untrusted.

New certificate templates

Certificates (9)	
Fortinet_SSL_ECDSA384	C = US, CN = FGVM080000072178, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_Factory	C = US, CN = FortiGate, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL	C = US, CN = FGVM080000072178, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL_DSA1024	C = US, CN = FGVM080000072178, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL_DSA2048	C = US, CN = FGVM080000072178, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL_ECDSA256	C = US, CN = FGVM080000072178, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL_RSA1024	C = US, CN = FGVM080000072178, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_SSL_RSA2048	C = US, CN = FGVM080000072178, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = FortiGate
Fortinet_Wifi	C = US, CN = auth-cert.fortinet.com, L = Sunnyvale, O = Fortinet, ST = California, OU = FortiWifi
Local CA Certificates (2)	
Fortinet_CA_Untrusted	C = US, CN = Fortinet Untrusted CA, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate
Fortinet_CA_SSL	C = US, CN = FGVM080000072178, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate
External CA Certificates (3)	
Fortinet_CA	C = US, CN = support, L = Sunnyvale, O = Fortinet, ST = California, emailAddress = support@fortinet.com, OU = Certificate Authority
Fortinet_Wifi_CA	C = US, OU = (c) 2012 Entrust, Inc. - for authorized use only, O = Entrust, Inc., CN = Entrust Certification Authority - L1K
Fortinet_Wifi_CA2	C = US, OU = (c) 2009 Entrust, Inc. - for authorized use only, O = Entrust, Inc., CN = Entrust Root Certification Authority - G2

```
Murat_VM # config vpn certificate setting

Murat_VM (setting) # get
ocsp-status          : disable
ssl-ocsp-status      : disable
ssl-ocsp-option      : server
ocsp-default-server :
check-ca-cert        : enable
strict-crl-check     : disable
strict-ocsp-check    : disable
certname-rsa1024     : Fortinet_SSL_RSA1024
certname-rsa2048     : Fortinet_SSL_RSA2048
certname-dsa1024     : Fortinet_SSL_DSA1024
certname-dsa2048     : Fortinet_SSL_DSA2048
certname-ecdsa256    : Fortinet_SSL_ECDSA256
certname-ecdsa384    : Fortinet_SSL_ECDSA384
```

- These certificates are used to place private key of self generated certificates.
- By having these certificates, fortigate can self generate different key sizes and different certificate types.

VPN Features

RFC 7427 IKEv2 Digital Signature Authentication

```
FG3200D_DUT_195_78 (VD_2) # show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "test2"
        set interface "port28"
        set ike-version 2
        set authmethod signature
        set digital-signature-auth enable
        set signature-hash-alg sha2-512
        set remote-gw 10.27.255.254
        set certificate "IPSEC_Cert_2"
        set peer "CA_Peer"
    next
end
```

```
FG3200D_DUT_195_78 (test2) # set digital-signature-auth
enable     Enable IKEv2 Digital Signature Authentication (RFC 7427).
disable    Disable IKEv2 Digital Signature Authentication (RFC 7427).
```

- This document adds a new IKEv2 [RFC7296] authentication method to support signature methods in a more general way. The current signature-based authentication methods in IKEv2 are per algorithm, i.e., there is one for RSA digital signatures, one for DSS digital signatures (using SHA-1), and three for different ECDSA curves, each tied to exactly one hash algorithm. This design is cumbersome when more signature algorithms, hash algorithms, and elliptic curves need to be supported:

IKEv2 Asymmetric authentication

```
FG3200D_DUT_195_78 (test2) # show
config vpn ipsec phase1-interface
    edit "test2"
        set interface "port28"
        set ike-version 2
        set authmethod signature
        set authmethod-remote psk
        set peertype any
        set digital-signature-auth enable
        set signature-hash-alg sha2-512
        set remote-gw 10.27.255.254
        set certificate "IPSEC_Cert_2"
    next
end

FG3200D_DUT_195_78 (test2) # set psksecret-remote
<passwd>    please input password value

FG3200D_DUT_195_78 (test2) # set psksecret-remote
```

- Why the feature introduced
  - » FortiOS has always provided a single authmethod configuration, either psk or signature, and both sides of the AUTH exchange would use the same auth method. This ECO introduces a new phase1 option, authmethod-remote, that can be changed independently of authmethod. The default for authmethod-remote is unset, which retains the current, symmetric auth behavior. When authmethod-remote is set to either psk or signature, the IKEv2 auth verify callback function in iked is changed to the appropriate auth method, hence enabling the asymmetric behavior. When authmethod-remote is set to psk, another new setting, psksecret-remote, is visible, allowing the use of different pre-shared secrets in each direction.

RFC 7383 IKEv2 Message Fragmentation

```
FG3200D_DUT_195_78 (VD_2) #
FG3200D_DUT_195_78 (VD_2) # config vpn ipsec phase1-interface

FG3200D_DUT_195_78 (phase1-interface) # edit test2

FG3200D_DUT_195_78 (test2) #
FG3200D_DUT_195_78 (test2) # set fragmentation
enable     Enable intra-IKE fragmentation support on re-transmission.
disable    Disable intra-IKE fragmentation support.

FG3200D_DUT_195_78 (test2) # set fragmentation enable

FG3200D_DUT_195_78 (test2) # set fragmentation-mtu
fragmentation-mtu    Enter an integer value from <500> to <16000> (default = <1200>).

FG3200D_DUT_195_78 (test2) # set fragmentation-mtu
```

- Why
  - » The solution to the problem described in this document is to perform fragmentation of large messages by IKEv2 itself and replace them with a series of smaller messages. In this case, the resulting IP datagrams will be small enough so that no fragmentation at the IP level will take place. The primary goal of this solution is to allow IKEv2 to operate in environments that might block IP fragments. This goal does not assume that IP fragmentation should be avoided completely, but only in those cases when it interferes with IKE operations.

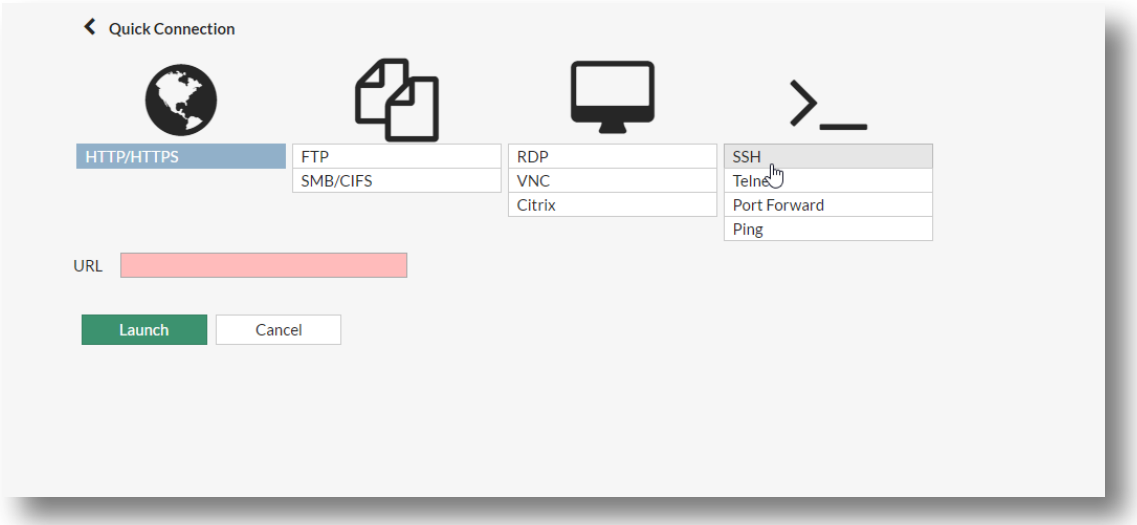
Allow peertype dialup for IKEv2 PSK dyanmic phase1

```
Murat_VM # show vpn ipsec phase1-inter
config vpn ipsec phase1-interface
    edit "To600D"
        set interface "port1"
        set ike-version 2
        set peertype any
        set localid "toto"
        set remote-gw 192.168.195.196
        set psksecret ENC [illegible]4i1G0LR
vTDQ/RiFdmY/z+uYp/MBXk8gjlghkjc027HOeJ
    next
end

Murat_VM # show vpn ipsec phase2-inter
config vpn ipsec phase2-interface
    edit "Ph2"
        set phase1name "To600D"
        set src-subnet 172.16.3.0 255.
    next
end
```

```
FGT6HD3916801566 (root) # show user local toto
config user local
    edit "toto"
        set type password
        set passwd-time 2017-04-21 02:41:01
        set passwd ENC cJMeysNyxXiAKv9YFYrKdNqKLEf5sClwRG9hxVL
72gdXXF[illegible]pr2dL+ViiTHfQry3+cGywRWBxD8HKK1mTFHTHRK7ALn+/BKFwfF
    next
end

FGT6HD3916801566 (root) # show user group
config user group
    edit "SSO_Guest_Users"
    next
    edit "Guest-group"
        set member "guest"
    next
    edit "DialupUser"
        set member "toto"
    next
end

FGT6HD3916801566 (root) # show vpn ipsec phase1-interface
config vpn ipsec phase1-interface
    edit "IPSEC_IKEv2"
        set type dynamic
        set interface "mgmt1"
        set ike-version 2
        set peertype dialup
        set usrgrp "DialupUser"
        set psksecret ENC PeSUbLnBUghFaVFOS1NW77YQ/4ssa7qm0Mzt+
stKNnaO40QgPYZ36RIspKkVYt7ueP9VrCDkytLHFs590io3EmD4fgpU4ONf9Wn
    next
end

FGT6HD3916801566 (root) # show vpn ipsec phase2-interface
config vpn ipsec phase2-interface
    edit "Ph2"
        set phase1name "IPSEC_IKEv2"
    next
end
```

- We already using peertype dialup with IKEv1. This change will allow to use the same on IKEv2.
- Idea behind this feature is, allow admin create a single Ph1 on Hub site and Site2Site Connections on remote locations.
- Every site will use it is own pre-shared key and Hub site will validate the pre-shared key based on user group

SSL VPN HTML 5 support



- Project of moving SSL VPN portal mode applications out from JAVA and made them available for HTML5 is started with RDP & VNC in 5.4
- This change now add the support for SSH and telnet application based on HTML5

Other features

Implement SSD Trim for log disk

```
FGT3KD_179_root # config system global

FGT3KD_179_root (global) # set ssd
ssd-trim-freq       SSD trim frequency.
ssd-trim-hour       Time of day to run ssd trim(hour part, 24 hour clock).
ssd-trim-min        Time of day to run ssd trim (min: 0-59, 60 for random).
ssd-trim-weekday    Day of week to run ssd trim.

FGT3KD_179_root (global) # set ssd-trim-freq
never      Never Run SSD Trim.
hourly     Run SSD Trim Hourly.
daily      Run SSD Trim Daily.
weekly     Run SSD Trim Weekly.
monthly    Run SSD Trim Monthly.

FGT3KD_179_root (global) # show full-configuration | grep ssd
    set ssd-trim-freq weekly
    set ssd-trim-hour 1
    set ssd-trim-min 60
    unset ssd-trim-weekday

FGT3KD_179_root (global) #
```

- What is trim in SSD?
  - A **trim** command (known as **TRIM** in the ATA command set, and UNMAP in the SCSI command set) allows an operating system to inform a **solid-state drive** (**SSD**) which blocks of data are no longer considered in use and can be wiped internally. **Trim** was introduced soon after **SSDs** were introduced.

NAT Session monitoring

```
FG3200D_DUT_195_78 (Traffic) # diagnose firewall ippool-all list
vdom:Traffic owns 1 ippool(s)
name:Customer
type:port-block-allocation
nat-ip-range:55.55.55.24-55.55.55.200


FG3200D_DUT_195_78 (Traffic) # diagnose firewall ippool-all stats
vdom:Traffic owns 1 ippool(s)
name: Customer
type: port-block-allocation
startip: 55.55.55.24
endip: 55.55.55.200
total ses: 0
tcp ses: 0
udp ses: 0
other ses: 0


FG3200D_DUT_195_78 (Traffic) # diagnose firewall ippool-all
list     list
stats    statistics
```

- Why
  - » Giving more visibility to NAT pooling

Device detection (Servers)

```
Murat_VM # diagnose user device list
hosts
  vd root/0  00:0c:29:bb:29:fd  gen 32  req S/2
    created 100948s  gen 8  seen 5s  port2  gen 22
    ip 10.2.255.1
    type 7 'Fortinet Device'  src configured  id 0  gen 6
  vd root/0  00:0c:29:2a:dc:f9  gen 79  req S/2
    created 101974s  gen 1  seen 3s  port3  gen 68
    ip 172.16.3.1
    type 12 'Linux PC'  src configured  id 0  gen 7
  vd root/0  00:0c:29:42:e5:62  gen 80  req 0
    created 101675s  gen 4  seen 1707s  port2  gen 69
    ip 10.2.255.200
    type 12 'Linux PC'  src configured  id 0  gen 8
    server ftp
```

- Extension of device detection. Allow to detect Servers and view server traffic on Fortiview

Long VDOM Name Support

» To allow admin creating VDOM names longer then 11 characters

```
Summary: enable/disable long vdome support
Detail: config system global
    set long-vdom-name enable/disable # default is disable. help text: Enable/disable long vdom name support."
end

Status: Change
Summary: can specify both long and short vdom name when creating a vdom
Detail: config vdom
    edit long-vdname/short-vdname # this is mainly designed to be used by FMG when FMG needs to install config to FGT
end
```

Internet service database on Firewall policies

```
Murat_VM (0) # set Murat_VM (0) # set
name                        Policy name.
uuid                        Universally Unique IDentifier.
*srcintf                     Incoming (ingress) interface.
*dstintf                     Outgoing (egress) interface.
srcaddr                     Source address and address group names.
internet-service            Enable/disable use of Internet Services for this policy. If enabled, destination a
internet-service-id         Internet Service ID.
internet-service-custom     Custom Internet Service Name.
rtp-nat                     Enable Real Time Protocol (RTP) NAT.
learning-mode               Enable to allow everything, but log all of the meaningful data for security inform
action                      Policy action (allow/deny/ipsec).
send-deny-packet            Enable to send a reply when a session is denied or blocked by a firewall policy.
status                      Enable or disable this policy.
schedule                    Schedule name.
schedule-timeout            Enable to force current sessions to end when the schedule object times out. Disabl
logtraffic                  Enable or disable logging. Log all sessions or security profile sessions.
logtraffic-start            Record logs when a session starts and ends.
session-ttl                 Session TTL in seconds for sessions accepted by this policy. 0 means use the syste
vlan-cos-fwd                VLAN forward direction user priority: 255 passthrough, 0 lowest, 7 highest.
vlan-cos-rev                VLAN reverse direction user priority: 255 passthrough, 0 lowest, 7 highest..
wccp                        Enable/disable forwarding traffic matching this policy to a configured WCCP server
groups                      Names of user groups that can authenticate with this policy.
users                       Names of individual users that can authenticate with this policy.
devices                     Names of devices or device groups that can be matched by the policy.
natip                       Policy-based IPsec VPN: source NAT IP address for outgoing traffic.
match-vip                   Enable to match packets that have had their destination addresses changed by a VIP
diffserv-forward            Enable to change packet's DiffServ values to the specified diffservcode-forward va
diffserv-reverse            Enable to change packet's reverse (reply) DiffServ values to the specified diffser
tcp-mss-sender              Sender TCP maximum segment size (MSS).
tcp-mss-receiver            Receiver TCP maximum segment size (MSS).
```

- Used as destination.

Support MAC authentication

```
Murat_VM # config firewall policy

Murat_VM (policy) # edit 0
new entry '0' added

Murat_VM (0) # set radius-mac-auth-bypass
enable      Enable MAC authentication bypass.
disable     Disable MAC authentication bypass.
```

```
Murat_VM # config system interface

Murat_VM (interface) # edit port8

Murat_VM (port8) # set security-mode
none               No security option.
captive-portal     Captive portal authentication.

Murat_VM (port8) # set security-mode captive-portal

Murat_VM (port8) # set security-mac-auth-bypass
enable      Enable MAC authentication bypass.
disable     Disable MAC authentication bypass.
```

- The idea is to allow user already authenticated in a shop wont authenticate again. The authentication will be done based on MAC address of the host transparently.

VxLAN Support

```
Murat_VM # config system vxlan

Murat_VM (vxlan) # edit 1
new entry '1' added

Murat_VM (1) # get
name                  : 1
interface             :
vni                   : 0
ip-version            : ipv4-unicast
dstport               : 4789
remote-ip             :


Murat_VM (1) # set
*interface      Local outgoing interface.
*vni            VXLAN network ID.
*ip-version     IP version to use for VXLAN device.
*remote-ip      Remote IPv4 address of VXLAN.
dstport        VXLAN destination port (default = 4789).
```

- This allow to forward packets with VxLAN header to other VTEPs either Multicast or Unicast.

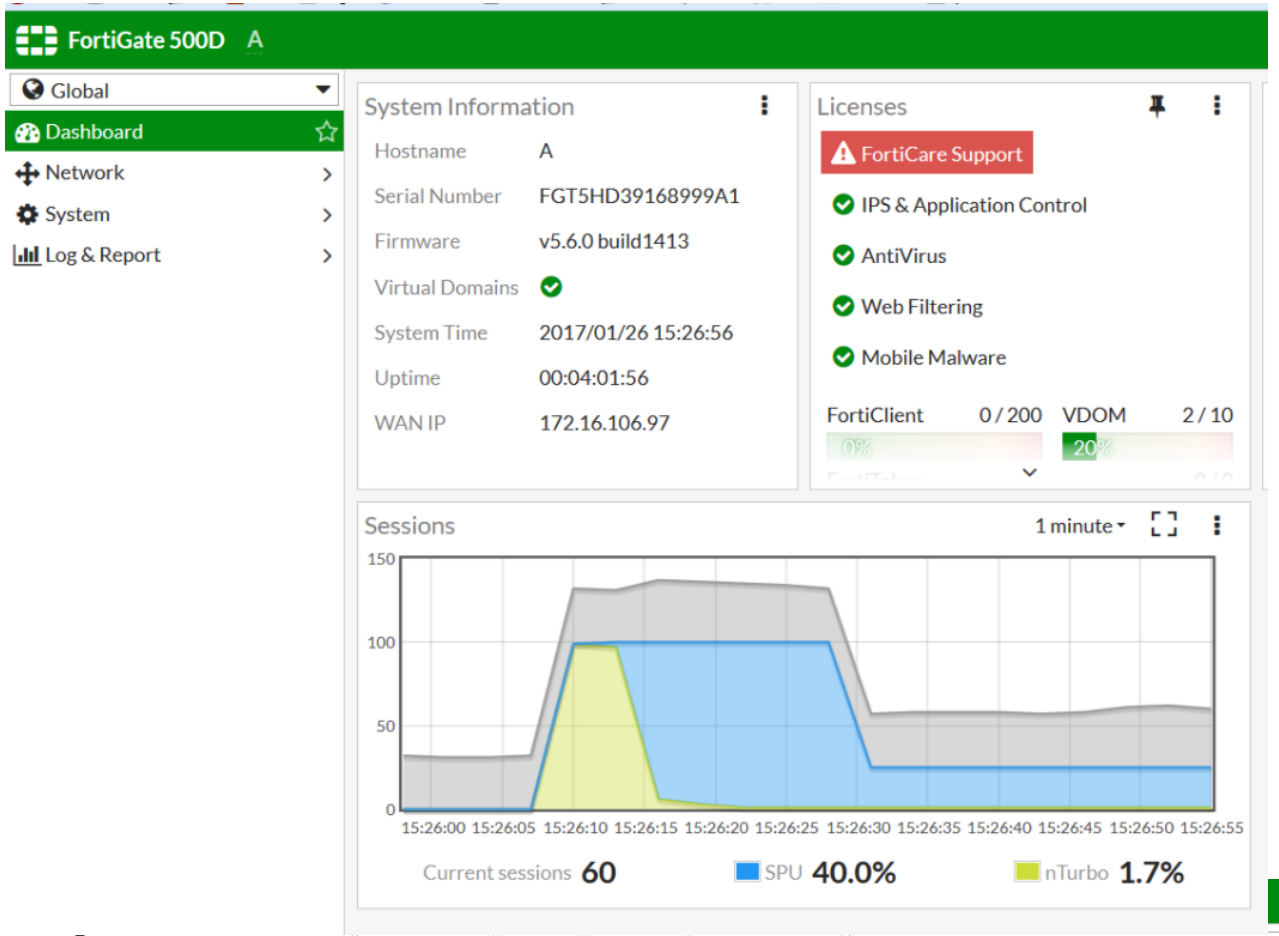
Debug improvements

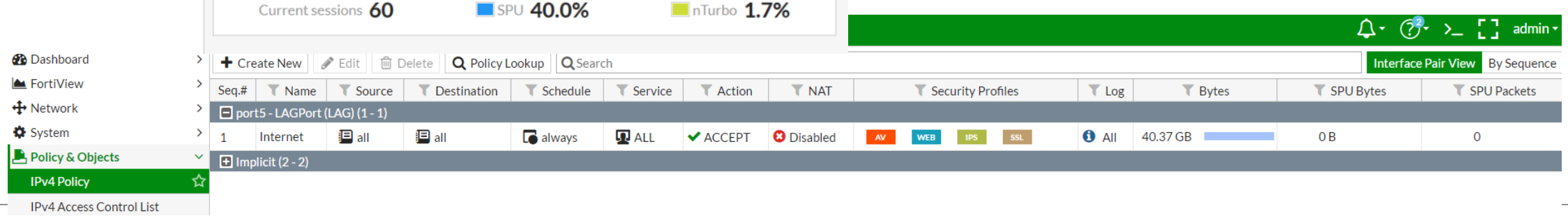
» Debug will run fix period of time and then disabled automatically.

```
Murat_VM # diagnose debug application fnbamd  -1
Debug messages will be on for 30 minutes.
```

```
Murat_VM # diagnose debug duration >
<Integer>    Duration in minutes, min = 1, max = 4294967295, 0 means unlimited.
```

Improve usability





- More visibility on traffic handled by SPUs (NP and Nturbo)

Support Multicast HA

```
Murat_VM (ha) # show full-configuration
config system ha
    set group-id 0
    set group-name ''
    set mode standalone
    set password ENC QjZtKFXI+Q5Ot6qgPz+IqEvfN3HighkS5D7
EpIZgDoHbD/8paU/jvpXKQlVbNV1FQj+HQ==
    set hbdev "port4" 50
    unset session-sync-dev
    set route-ttl 10
    set route-wait 0
    set route-hold 10
    set multicast-ttl 600
    set sync-config enable
    set encryption disable
    set authentication disable
    set hb-interval 2
    set hb-lost-threshold 20
    set hello-holddown 20
    set gratuitous-arps enable
    set arps 5
    set arps-interval 8
    set session-pickup disable
    set session-sync-daemon-number 1
    set link-failed-signal disable
    set uninterruptible-upgrade enable
    set ha-eth-type "8890"
    set hc-eth-type "8891"
    set l2ep-eth-type "8893"
    set ha-uptime-diff-margin 300
    set standalone-config-sync disable
    set override disable
    set priority 128
    unset monitor
    unset pingserver-monitor-interface
    set pingserver-failover-threshold 0
    set pingserver-slave-force-reset enable
    set pingserver-flip-timeout 60
    unset vdom
end
```

- Multicast routing table was not synchronized before causing high failover time during HA failover.
- This change allow to synchronize multicast routes.

New Conserve Mode settings

```
Technical Details: The following changes were made in this ECO.
1. Implemented CLI commands to configure "extreme", "red", and "green"
   memory usage thresholds in percentages of total RAM.
   Note that we use the notion of "memory used" for these thresholds,
   and set them to 95% (extreme), 88% (red) and 82% (green).
2. Removed structure av_conserve_mode, other changes in kernel to obtain and
   set memory usage thresholds from the kernel
3. Added conserve mode diagnostic command "diag hardware sysinfo conserve",
   which prints information about memory conserve mode.
4. Fixed conserve mode logs in the kernel
5. Added converve mode stats to the proxy daemon
   (via command "diag sys proxy stats all | grep conserve_mode")
```

- This is to clarify Conserve mode and the output of the conserve mode.

```
Murat_VM # config system global

Murat_VM (global) # set mem
memory-use-threshold-extreme    Threshold at which memory usage is considered extreme (new sessions are dropped) (% of total RAM, default = 95).
memory-use-threshold-green      Threshold at which memory usage will force system to exit conserve mode (% of total RAM, default = 82).
memory-use-threshold-red        Threshold at which memory usage will force system to enter conserve mode (% of total RAM, default = 88).
```

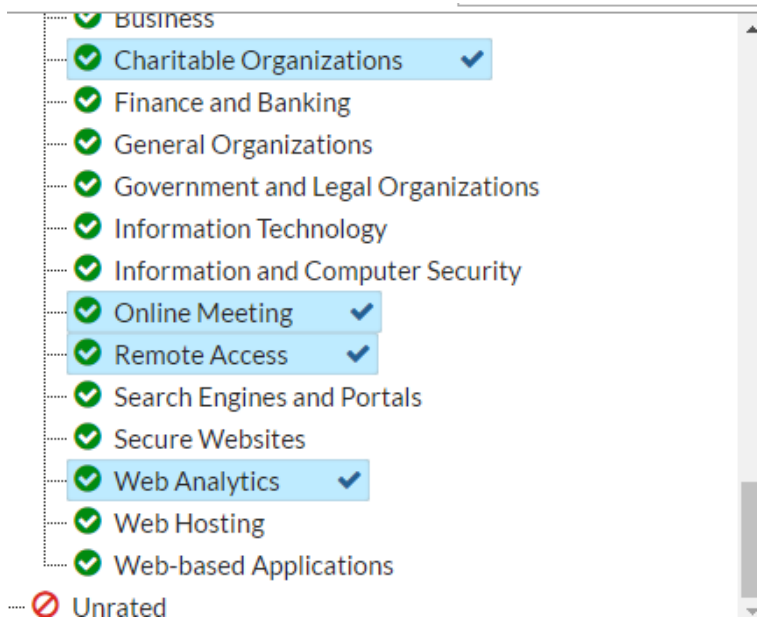
Safe search for DNS Profile

```
Murat_VM # config dnsfilter profile

Murat_VM (profile) # edit default

Murat_VM (default) # set safe-search
disable    Disable safe search for Google/Bing/YouTube.
enable     Enable safe search for Google/Bing/YouTube.
```

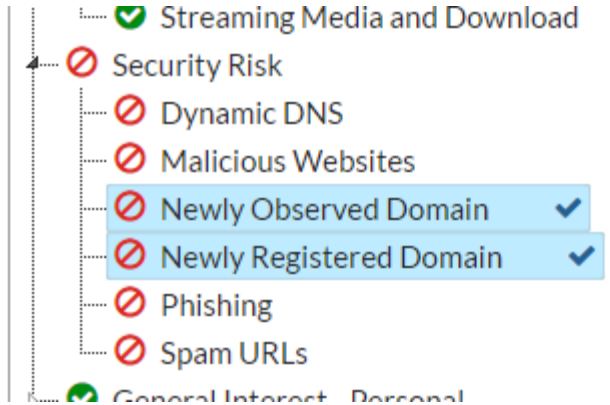
- Safe search on search engines can be enforced by DNS.
- This feature allow to enforce safe search on popular Search engines when DNS profile in use (Proxy mode)

Fortiguard version 8

```
Technical Details:

New added categories for FortiGuard Service v8.0:
5.90=Newly Observed Domain
5.91=Newly Registered Domain
7.92=Charitable Organizations
7.93=Remote Access
7.94=Web Analytics
7.95=Online Meeting
```



- Fortiguard web filtering now have new categories and this feature is the support on the FOS side.




FORTINET